Министерство образования Республики Беларусь

Учебно-методическое объединение по естественнонаучному образованию

УТВЕРЖДАЮ
Первый заместитель Министра образования Республики Беларусь
_____ А.И. Жук
30.04.2012
(дата утверждения)
Регистрационный № ТД-Р.397/тип.

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Типовая учебная программа
для учреждений высшего образования по направлению специальности

1-98 01 01 - 01 Компьютерная безопасность (математические методы и программные системы)

СОГЛАСОВАНО
Председатель учебно-методического объединения по естественнонаучному образованию
_____ А.Л. Годлевский
28.03.2012
(дата)

СОГЛАСОВАНО
Зам. начальника управления высшего и среднего специального образования Министерства образования Республики Беларусь
_____ Э.Г. Шевцов
(И.О. Фамилия)
30.04.2012
(дата)

Проректор по учебной и воспитательной работе Государственного учреждения образования «Республиканский институт высшей школы»
_____ В.И. Шупляк
(И.О. Фамилия)
02.04.2012
(дата)

Эксперт-нормоконтролер
_____ Н.В. Сенько
02.04.2012
(дата)

Минск 2012

Техническая совет информационной безопасности

СОСТАВИТЕЛИ:
Ю.И. Иванченко, профессор кафедры технологий программирования Белорусского государственного университета, кандидат технических наук.

РЕЦЕНЗЕНТЫ:
Кафедра информационных технологий в управлении Белорусского национального технического университета;

В.Н. Ярмолик, профессор кафедры программного обеспечения информационных технологий Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», доктор технических наук, профессор.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ В КАЧЕСТВЕ ТИПОВОЙ:

Кафедрой технологий программирования Белорусского государственного университета
(протокол № 10 от 17.02.2011г.);

Научно-методическим советом Белорусского государственного университета
(протокол № 2 от 21.02.2011г.);

Научно-методическим советом по компьютерной безопасности Учебно-методического объединения по естественнонаучному образованию
(протокол № 7 от 23.03.2011г.)

Ответственный за выпуск: Ю.И. Иванченко

Пояснительная записка

Дисциплина «Теоретические основы информационной безопасности» ориентирована на обучение студентов базовым знаниям, умениям и навыкам в области защиты информации. Изучаемые темы представляются на основе современной нормативной регулятивной базы и национального законодательства.

Изучение теоретических основ информационной безопасности преследует следующие цели: обучение студентов основам построения и использования современных защищенных информационных компьютерно-коммуникационных систем, подготовку специалистов, умеющих создавать защищенные информационные системы и исследовать защищенность компьютерно-коммуникационных систем.

При этом требуется разрешить две основные задачи: во-первых, дать студентам базовые знания в области информационной безопасности и, во-вторых, сформировать системное понимание проблем безопасности и путей их решения.

При построении курса «Теоретические основы информационной безопасности» использовались современные представления о процессах жизненного цикла информационных систем и парадигма информационной безопасности.

Дисциплина «Теоретические основы информационной безопасности» непосредственно связана с изучаемыми дисциплинами специализации.

Сформированные компетенции в области защиты информации являются базовыми при изучении всех последующих дисциплин специализации, при выполнении курсовых и дипломных работ.

В результате изучения дисциплины студенты должны

знать:

– терминологию в области информационной безопасности;

– современные методы и механизмы защиты информации;

– методологии проектирования и оценки соответствия систем защиты информации;

– стандарты по информационной безопасности;

уметь:

– использовать стандарты при создании и для оценки защищенных систем;

– применять методологии проектирования и оценки соответствия систем защиты информации.

На лекционных занятиях по дисциплине «Теоретические основы информационной безопасности» возможно использование элементов проблемного обучения: проблемное изложение некоторых аспектов, использование частично-поискового метода.

Условия для самостоятельной работы студентов, в частности, для развития навыков самоконтроля, способствующих интенсификации учебного процесса, обеспечиваются:

- наличием и использованием в учебном процессе открытых систем автоматизированного тестирования, которые доступны пользователям через Интернет в любое удобное для них время;

- наличием и полной доступностью электронных (и бумажных) вариантов курсов лекций и учебно-методических пособий по основным разделам дисциплины.

В соответствии с типовым учебным планом по направлению специальности 1-98 01 01-01 Компьютерная безопасность (математические методы и программные системы) программа предусматривает для изучения дисциплины всего 95 учебных часов, в том числе 34 часа аудиторных занятий: лекции – 26 часов, лабораторные занятия – 8 часов.

Примерный тематический план

№	Название раздела, темы	Количество аудиторных часов		
		Всего	В том числе	
			Лекции	Лабораторные занятия
	Раздел I.			
1.	Введение	2	2	
2.	Основы информационной грамоты	2	2	
3.	Информационное обеспечение деятельности	2	2	
4.	Правовое обеспечение деятельности в области информационных технологий и безопасности	2	2	
	Раздел II. Парадигма безопасности			
5.	История и современная парадигма информационной безопасности	2	2	
6.	Угрозы безопасности информационно-коммуникационных технологий	2	2	
7.	Уязвимости информации и информационных систем	2	2	
	Раздел III. Анализ защищенности			
8.	Методы исследования проблем защиты информации	2	2	
9.	Методология оценки защищенности	4	2	2
	Раздел IV. Менеджмент информационной безопасности			
10.	Принципы построения систем защиты информации	6	4	2
11.	Политика информационной безопасности	4	2	2
12.	Менеджмент информационной безопасности	4	2	2
	Всего	34	26	8

Содержание

Раздел I.

1. Введение

Ведение в специализацию. Предмет, цели и задачи курса. Содержание дисциплины. Информационная безопасность и защита информации. Термины и определения.

2. Основы информационной грамоты.

Основные понятия. Термины и определения. Система показателей, характеризующих информацию. Качество информации и его обеспечение.

3. Информационное обеспечение деятельности

Информационное обеспечение деятельности (бизнеса). Документоведение. Документационное обеспечение управления. Общая характеристика процессов сбора, передачи, обработки и накопления информации. Управление знаниями.

4. Правовое обеспечение деятельности в области информационных технологий и безопасности

Правовое обеспечение защиты информации. Классификация правовых актов. Правовые акты ориентированные на защиту информации. Конституционное законодательство. Общие законы, кодексы, которые включают нормы по вопросам информатизации и информационной безопасности. Специальные законы (О государственных секретах, Об информации, информатизации и защите информации). Подзаконные акты. Правоохранительное законодательство (Гражданский кодекс, Уголовный кодекс, Уголовно-процессуальный кодекс)

Нормативное обеспечение защиты информации. Стандарты информационной безопасности США, Германии, Великобритании, Российской Федерации, ISO. Технические нормативные правовые акты Республики Беларусь.

Раздел II. Парадигма безопасности

5. История и современная парадигма информационной безопасности

Возникновение и история развития проблемы защиты информации. Структура теории компьютерной безопасности. Методологические основы защиты информации. Суть системно-концептуального подхода. Парадигма информационной безопасности.

6. Угрозы безопасности информационно-коммуникационных технологий

Угрозы безопасности информационно-коммуникационных технологий. Классификация умышленных угроз. Общая классификация угроз. Анализ угроз информационной безопасности информационно-коммуникационных технологий. Система дестабилизирующих факторов, влияющих на уязвимость информации. Методология формирования полного множества угроз. Основные методы реализации угроз. Причины, виды и каналы утечки информации.

7. Уязвимости информации и информационных систем

Уязвимость информации и информационных систем. Система показателей уязвимости. Методы и модели оценки уязвимостей.

Раздел III. Анализ защищенности

8. Методы исследования проблем защиты информации

Общая характеристика методов исследования проблем защиты информации. Основные положения теории нечетких множеств. Основные положения нестрогой математики. Неформальные методы оценивания. Неформальные методы поиска оптимальных решений.

9. Методология оценки защищенности

Оценка защищенности средств информатизации и ИТ-систем. Общие критерии оценки защищенности. Функциональные и гарантийные требования.

Раздел IV. Менеджмент информационной безопасности

10. Принципы построения систем защиты информации

Системы защиты информации. Общеметодологические принципы построения систем защиты информации. Основы архитектурного построения. Модели систем и процессов защиты информации. Модели разграничения доступа к информации. Общее содержание основных вопросов организации и обеспечения работ по защите информации. Структура и функции органов защиты информации.

11. Политика информационной безопасности

Понятие политики безопасности. Основные типы и содержание политик безопасности.

12. Менеджмент информационной безопасности

Системы менеджмента безопасности информации. Правила и требования. Управление рисками. Аудит информационной безопасности.

Информационно-методическая часть

Литература

Основная

1. Астахов А. Искусство управления информационными рисками. – М.: Издательство ДМК, 2010. – 312с.
2. Герасименко В.А. Защита информации в АСОД. М.: Энергоатомиздат, 1994, Кн. 1, 2.
3. Герасименко В.А. Основы информационной грамоты. – М.: Энергоатомиздат, 1996. – 320 с., ил.
4. Герасименко В.А., Малюк А.А. Основы защиты информации. М.: ООО “Инкомбук”, 1997.
5. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – К.:ООО "ТИД "ДС", 2001. – 688 с.
6. Курило А.П., Зефиров С.Л., Голованов В.Б. и др. Аудит информационной безопасности. – М.: Издательская группа «БДЦ-пресс», 2006. – 304 с.
7. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: Учебное пособие. СПб.: Питер, 2008.
8. В. Л. Цирлов. Основы информационной безопасности: краткий курс. – Ростов н/Д: Феникс, 2008. – 253с. – (Професиональное образование).
9. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебн. Пособие. – М.:ИД "Форум": ИНФРА-М, 2009. – 416 с.:ил. –

(Профессиональное образование)
10. СТБ П ИСО/МЭК 17799-2000/2004 Информационные технологии и безопасность. Правила управления информационной безопасностью.
11. СТБ П ИСО/МЭК 27001-2008 Информационные технологии. Технологии безопасности. Системы управления защитой информации. Требования.
12. СТБ 34.101.1-2004 Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
13. СТБ 34.101.2-2004 Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
14. СТБ 34.101.3-2004 Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности.
15. Закон Республики Беларусь Об оценке соответствия требованиям технических нормативных правовых актов в области технического нормирования и стандартизации.
16. Стандарты ISO серии 27000.

Дополнительная

17. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности. Учебн. Пособие для вузов. М.:Радио и связь, 2000.-192с.:ил.
18. Сёмкин С.Н., Беляков Э.В., Гребнев С.В., Козачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации. М.:Гелиос АРВ, 2005. – 192с.
19. [Электрон. ресурс] - http://www.pravo.by
20. [Электрон. ресурс] - www.gosstandart.gov.by
21. [Электрон. ресурс] - http://www.iso.ch
22. [Электрон. ресурс] - https://ssl.bsi.bund.de/english/gshb/manual/t/t03.htm
23. [Электрон. ресурс] - http://www.intuit.ru/
24. [Электрон. ресурс] - www.ivanchenko.by

– Текущий контроль по дисциплине «Теоретические основы информационной безопасности» рекомендуется осуществлять в течение всего семестра в виде вопросов для самоконтроля и 1-2 контрольных работ (лекционная часть курса).

– Для закрепления и проверки знаний и умений студентов (практическая часть курса) рекомендуется разработать 5-6 индивидуальных заданий, которые предполагают подготовку и представление краткого сообщения по предложенной теме.

– Для контроля и самоконтроля знаний рекомендуется использовать в учебном процессе системы автоматизированного тестирования: инструменты с эффективной функциональностью контроля, тренинга и самостоятельной работы.

– Успеваемость студентов в рамках дисциплины «Теоретические основы информационной безопасности» рекомендуется оценивать в конце семестра в форме экзамена.